REMARKS

Claim Status

Claims 1-4, 9-18, 20 and 22-28 are now pending, with claims 1, 10-18 and 28 being in independent form. Claims 5-8, 19 and 21 have been canceled. Claims 1-4, 9, 10, 12, 14, 16, 18 and 20 have been amended. Independent claim 28 and dependent claims 22-27 have been added. The amendments to claims 2, 6, 9 and 10 are merely cosmetic or clarifying in nature. Support for new dependent claims 25, 26 and 27 may be found, for example, at pg. 13, lines 25-29 of the specification as originally filed. No new matter has been added. Reconsideration of the application, as herein amended, is respectfully requested.

Overview of the Office Action

The specification has been objected to for allegedly failing to provide antecedent basis for the claimed subject matter. Withdrawal of this objection is in order, as explained below.

Claims 4 and 7 have been objected to based on a minor informality. Withdrawal of this objection is in order, as also explained below.

Claim 6 stands rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Claim 6 has been canceled. This rejection is therefore moot.

Claims 1-21 stand rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 6,845,447 ("*Fujioka*") in view of EP 0 139 313 ("*Chaum*").

Applicants have carefully considered the Examiner's rejections and the comments provided in support thereof. For the following reasons, applicants respectfully assert that all claims now presented for examination in the instant application are patentable over the cited art.

Amendments Addressing Formalities

The Examiner (at pg. 2 of the Office Action) has objected to claims 12, 14, 16 and 18 because they recite "a computer readable medium" and the "specification does provide proper antecedent basis for such a claim limitation".

In the earlier Office Action of October 16, 2008, the Examiner provided applicants with suggested claim language to overcome an asserted Section 101 rejection. Applicants thank the Examiner for this previously suggested language. Applicants have now amended claims 12, 14, 16 and 18 to incorporate the Examiner's suggested language and to delete the term "computer readable medium" so that claims 12, 14, 16 and 18 each now recites "A computer program executing on a processor which, when used on a computer apparatus, causes...". Independent claims 12, 14, 16 and 18 now also recite that the computer program includes the program code for executing the corresponding features recited in claims 10, 13, 15 and 17, respectively.

In view of the foregoing, independent claims 12, 14, 16 and 18 as now amended are fully supported by the specification, and are fully in accordance with Section 101. Reconsideration and withdrawal of this objection are accordingly deemed to be in order.

The Examiner has objected to the dependency of claims 4 and 7 in that they are improper dependent claims. Dependent claim 7 has been canceled, and the objection to claim 7 is therefore moot. Dependent claim 4 has been amended to depend from dependent claim 3, and withdrawal of that objection is therefore deemed to be in order.

Patentability of the Independent Claims under 35 U.S.C. 103(a)

Independent claim 1 has now been amended to clarify the salient features of the claimed invention. That is, independent claim 1 has been amended to recite, *inter alia*, "establishing, at a trusted authority apparatus, a link between a data pair (x_i, y_i) comprising said data signal and said digital signature, and a signing session in which said data pair (x_i, y_i) was generated, the fair blind

signature scheme permitting establishment of the link via a tracing protocol included in the fair blind signature scheme". Thus, each independent claim clarifies or includes features associated with the use and implementation of a fair blind digital signature. No new matter has been added.

The Examiner (at pgs. 4-5 of the Office Action) acknowledges that *Fujioka* fails to teach "establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme" as recited in independent claim 1, and cites *Chaum* to provide these features.

Applicants disagree, however, that any combination of *Fujioka* and *Chaum* achieves the subject matter of now-amended independent claim 1, as well as independent claims 10-18. There is nothing in *Chaum* to cure the above-discussed deficiencies in *Fujioka* relating to the lack of teachings of applicants' claimed implementation of a fair blind digital signature as recited in each of independent claims 1 and 10-18.

Chaum teaches a system for blinding a signature (see Abstract). *Chaum* uses an example involving individuals named Bob and Alice sending each other messages to describe the principle of a "blind signature", and further explains the underlying theory for blinding a signature. With the blind (not fair blind) signature scheme of *Chaum*, a user obtains a digital signature of a message from a signer without providing the signer with information on the content of the message. Moreover, *Chaum* is disclosed and discussed at pg. 2, lines 13-18 of applicants' instant specification. *Chaum* fails to make any mention whatsoever of a **fair blind** signature scheme. Similarly to *Fujioka*, which simply describes a blind signature scheme, *Chaum* also discloses a blind signature scheme. The combination of *Fujioka* and *Chaum* thus fails to achieve the expressly recited subject matter of independent claims 1 and 10-18.

The claimed electronic voting system is based on the use of **fair blind** signatures. A **fair blind** signature scheme involves an additional participant (designated as a "trusted

authority") and, with the help of the trusted authority, a signer can identify which signature results from a given signing session. The skilled person would have no reason to modify the teachings of *Fujioka* to achieve these advantages and functionality in the manner achieved by applicants' claimed invention, absent impermissible hindsight reconstruction based on applicants' disclosure.

Fujioka teaches an electronic voting method involving voters (via voter apparatus), an administrator (via election administrator apparatus), and a counter (via counter apparatus). *Fujioka* describes an embodiment that uses several counters to prevent fraud (fraud is possible when there is only one counter apparatus that owns a secret key which is adapted to decrypt encrypted votes received from voter apparatus; this fraud allows the counter apparatus to obtain partial results of the voting session before the end of the vote).

The *Fujioka* method, however, is based on a blind signature scheme, not a **fair** blind signature scheme, which the Examiner has indeed recognized by citing *Chaum* in an effort to cure this deficiency of *Fujioka*. The voting process of *Fujioka* is explained in its abstract and its description of the voting procedure (see, e.g., pg. 6, lines 25 to col. 9, line 38, described in relation with Fig. 6).

In the claimed invention, a fair blind signature scheme allows the signer who generates the fair blind signature to identify which signature results from a given signing session. Such identification involves a trusted authority that applies a signature tracing algorithm (i.e., REV_J in applicants' instant specification). The trusted authority(ies) allow signers to identify which signature results from which signing session. This is made possible by the use of a fair blind signature scheme.

The claimed system and methods which implement a fair blind signature scheme not only allows voters to be traced when necessary (in a manner which maintains the secrecy of their vote), but also respect a "vote and walk away" principle which is not offered by the voting

system of *Fujioka*. The skilled person would have no reason to modify the system of *Fujioka* based on the teachings of *Chaum* to achieve a system and method that implement a fair blind signature scheme, because *Fujioka* and *Chaum* each simply disclose a blind signature scheme.

Fujioka and *Chaum* merely describe old, well-known blind signature techniques. There is no mention whatsoever in the entire disclosure of the *Fujioka* and *Chaum* patents of the word *fair* in association with *blind signature*, i.e., the words "fair blind signature" are not disclosed. *Fujioka* and *Chaum* thus fail to teach or suggest now amended independent claim 1, as well as dependent claims 10-18 which each recite the use of a fair blind signature scheme. *Fujioka* fails to teach or suggest the expressly recited subject matter of now amended independent claims 1 and 10-18.

Reconsideration and withdrawal of the rejection of independent claims 1 and 10-18 as anticipated by *Fujioka* under 35 U.S.C. §103 are accordingly deemed to be in order, and early notice to that effect is solicited.

New Independent Claim 28

New independent claim 28 recites the step of "obtaining from a signer apparatus, according to a fair blind signature scheme, a digital signature (y_i) of a data signal (x_i) generated from a voter apparatus, said digital signal comprising an encrypted vote (v_i) of a voter". Moreover, new independent claim 28 further recites that "the fair blind signature scheme includes a tracing protocol which can be implemented, at a trusted authority apparatus, to establish a link between a data pair (x_i, y_i) comprising said data signal and said digital signature, and a signing session in which said data pair (x_i, y_i) was generated". There is no corresponding feature in the combination of the cited art which provides this expressly recited subject matter.

Independent claim 1 recites, *inter alia*, "establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital

signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme". New independent claim 28 correspondingly recites this feature, i.e., that "the fair blind signature scheme includes a tracing protocol which can be implemented, at a trusted authority apparatus, to establish a link between a data pair (x_i, y_i) comprising said data signal and said digital signature, and a signing session in which said data pair (x_i, y_i) was generated". The Examiner acknowledged that *Fujioka* failed to teach this expressly recited subject matter of independent claim 1, which is now correspondingly recited in new independent claim 28. *Chaum* was previously cited to provide these features.

The combination of the cited art, however, fails to teach or suggest such a system and/or method associated with the use or implementation of a fair blind digital signature. As explained above with respect to independent claim 1, *Fujioka* simply describes a conventional blind signature scheme, and *Chaum* also discloses a conventional blind signature scheme.

The claimed electronic voting system recited in new independent claim 28 is based on the use of **fair blind** signatures. A **fair blind** signature scheme involves an additional participant (designated as a "trusted authority") and, with the help of the trusted authority, a signer can identify which signature results from a given signing session. The skilled person would have no reason to modify the teachings of *Fujioka* and *Chaum* to achieve these advantages and functionality in the manner achieved by applicants' claimed invention, absent impermissible hindsight reconstruction based on applicants' disclosure. New independent claim 28 is therefore patentable over *Fujioka* and *Chaum* that each merely recite the use of a conventional blind signature scheme.

Dependent Claims

In view of the patentability of independent claims 1 and 10-18, as well as new independent claim 28, for at least the reasons presented above, each of dependent claims 2-4, 9

and 20, as well as new dependent claims 22-27, is deemed to be patentable therewith over the prior art. Moreover, each of dependent claims 2-4, 9, 20 and 22-27 additionally includes features that serve to still further distinguish the claimed invention over the applied art.

Conclusion

Based on all of the above, applicants submit that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an early resolution of any outstanding issues.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By /Lance J. Lieberman/
Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: January 28, 2010